(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－152837

(43)公開日　平成７年(1995)６月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　17/60					
Ｇ０６Ｋ　19/07					
		8724－5Ｌ	Ｇ０６Ｆ　15/ 21	３４０　Ａ	
			Ｇ０６Ｋ　19/ 00	Ｎ	

審査請求　未請求　請求項の数13　ＦＤ　（全 15 頁）

(21)出願番号　特願平6－244919

(22)出願日　平成６年(1994)９月14日

(31)優先権主張番号　１２２６３１

(32)優先日　1993年９月17日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(72)発明者　リチャード　マンデルバウム
アメリカ合衆国、07726　ニュージャージー、マナラパン、ナヴァホ　ロード　15

(74)代理人　弁理士　三俣　弘文

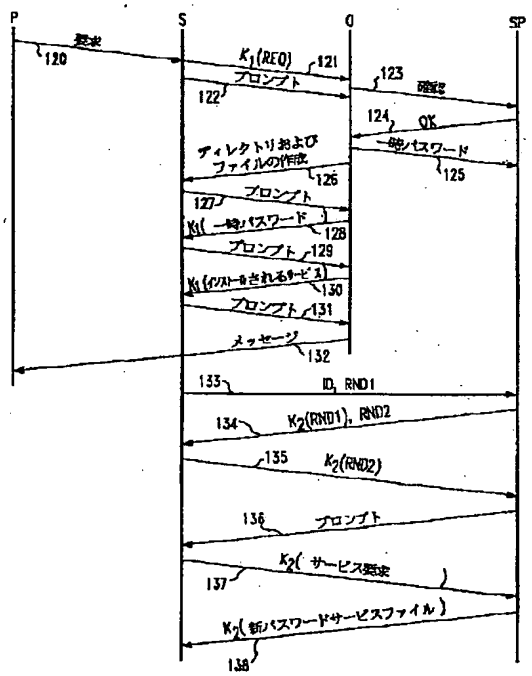
最終頁に続く

(54)【発明の名称】　スマートカード

(57)【要約】　（修正有）

【目的】　セキュリティの問題を克服し、リモート発給が可能であるような、複数のサービス提供者のサービスをのせたスマートカードを実現する。

【構成】　スマートカードは、発行者、保有者およびサービス提供者に関するメモリとプロセッサとを有し、さらに、発行者によってのみ制御される特性を有するファイルから始まるツリー状ファイル構造を有するオペレーティングシステムと、ツリー状ファイル構造の一部を形成しそれぞれ発行者によってのみ制御される特性を有する複数の実行可能ファイルを有する。オペレーティングシステムはさらに、発行者、保有者およびサービス提供者という各当事者に対応して、その当事者にのみアクセス可能であり、その当事者が実行可能ファイルにアクセス可能となる前にその当事者によってアクセスされる各当事者ごとのパスワードファイルを有する。



1

【特許請求の範囲】

【請求項１】　発行者／所有者、保有者およびサービス提供者に関するメモリとプロセッサとを有する多重アプリケーションスマートカードにおいて、

前記発行者／所有者によってのみ制御される特性を有するファイルから始まるツリー状ファイル構造を有するオペレーティングシステムと、

前記ツリー状ファイル構造の一部を形成し、それぞれ前記発行者／所有者によってのみ制御される特性を有し、参照されると前記メモリ内の許容データに作用するという意味で実行可能な複数の実行可能ファイルと、

前記発行者／所有者にのみアクセス可能であり、前記発行者／所有者が前記実行可能ファイルにアクセス可能となる前に前記発行者／所有者によってアクセスされるパスワードファイルと、

前記保有者にのみアクセス可能であり、前記保有者が前記実行可能ファイルにアクセス可能となる前に前記保有者によってアクセスされるパスワードファイルと、

前記サービス提供者にのみアクセス可能であり、前記サービス提供者が前記実行可能ファイルにアクセス可能となる前に前記サービス提供者によってアクセスされるパスワードファイルとからなることを特徴とする多重アプリケーションスマートカード。

【請求項２】　当事者と通信するように適合し、プロセッサを有するスマートカードにおいて、

ユーザエンティティごとに情報の格納および取得のための複数の論理ゾーンに配列され、その論理ゾーンのうちの少なくとも２つは、アクセス制御データを含むメモリセグメントを含むサブゾーンを有するメモリと、

前記当事者が、前記論理ゾーンのうちの所定の論理ゾーンに含まれるアクセス制御データに関係する情報をスマートカードに送ったときにのみ、その所定の論理ゾーンに、そのサブゾーンも含めて、前記当事者がアクセスすることを可能にする制御手段とからなることを特徴とするスマートカード。

【請求項３】　第１当事者によってのみ制御される属性を有するディレクトリファイルから始まるツリー状ファイル構造を有するオペレーティングシステムと、そのツリー状ファイル構造の一部を形成し前記第１当事者によってのみ制御される属性をそれぞれ有し参照されるとメモリ内の許容データに作用するという意味で実行可能な複数の実行可能ファイルと、前記第１当事者が前記実行可能ファイルにアクセスすることができる場合にのみアクセス可能なパスワードファイルとからなる、前記第１当事者によって発行されるスマートカードに対して、第２当事者がそのスマートカードの保有者にサービスを提供する機能をインストールする方法において、

前記保有者が、前記スマートカードと前記第１当事者の間の通信を確立するのを支援するステップと、

前記パスワードファイル内の含まれるデータを使用して、前記スマートカードと前記第１当事者の間のログインプロトコルを実行するステップと、

前記第２当事者のために前記スマートカード上にサービス機能をインストールする要求を前記第１当事者に通信する要求通信ステップと、

前記第１当事者が、前記ツリー状ファイル構造の一部を形成するように前記スマートカード内のユーザパスワードファイルを設定するステップと、

前記第１当事者が、前記ユーザパスワードファイルにデータを挿入するステップと、

前記第１当事者が、前記第２当事者にのみアクセス可能にするように前記ユーザパスワードファイルのファイル属性を変更するステップとからなることを特徴とする、スマートカードのインストール方法。

【請求項４】　前記ユーザパスワードファイルに格納されたデータについて前記第２当事者に通知するステップをさらに有することを特徴とする請求項３の方法。

【請求項５】　前記要求通信ステップの後に、前記第１当事者によって、前記要求が満たされることを前記第２当事者に確認するステップをさらに有することを特徴とする請求項３の方法。

【請求項６】　前記通信が電気通信網を使用することを特徴とする請求項３の方法。

【請求項７】　当事者が個人情報装置と通信する方法において、

前記個人情報装置が、チャレンジ・応答シーケンスによって前記当事者を認証する第１認証ステップと、

前記当事者が、チャレンジ・応答シーケンスによって前記個人情報装置を認証する第２認証ステップとからなることを特徴とする通信方法。

【請求項８】　前記第２認証ステップが前記第１認証ステップに先行することを特徴とする請求項７の方法。

【請求項９】　個人情報装置の保有者が、チャレンジ・応答シーケンスによって個人情報装置に認証されるステップをさらに有することを特徴とする請求項７の方法。

【請求項１０】　前記第２認証ステップが開始されるときに前記第１認証ステップが未了であることを特徴とする請求項７の方法。

【請求項１１】　前記第１認証ステップは、

前記個人情報装置が、ＩＤ情報および第１データストリングを含むチャレンジを送信するステップと、

前記個人情報装置によって送信されたＩＤ情報に基づく第１暗号化キーを使用して前記第１データストリングを暗号化し、暗号化した第１データストリングを前記個人情報装置に送信するステップとからなり、

前記第２認証ステップは、

前記当事者が、第２データストリングを含むチャレンジを送信するステップと、

前記個人情報装置に事前に格納されている第２暗号化キーを使用して前記第２データストリングを暗号化し、暗

号化した第２データストリングを前記当事者に送信するステップと、
前記当事者が、前記第２暗号化キーによって前記個人情報装置の真正を確認するステップと、
前記当事者が、前記第２暗号化キーによって前記個人情報装置を認証するステップとからなることを特徴とする請求項７の方法。
【請求項１２】　前記第１データストリングおよび前記第２データストリングはランダムシーケンスからなることを特徴とする請求項１１の方法。
【請求項１３】　前記第１暗号化キーと前記第２暗号化キーは同一であることを特徴とする請求項１１の方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、スマートカードに関する。
【０００２】
【従来の技術】マイクロエレクトロニクスにおける進展により、小さい空間内に多大な計算能力を備えることが可能となっている。実際、クレジットカード内に実質的にコンピュータ全体を入れることが可能となっており、これによって「スマートカード」が作成されている。スマートカードの大きな処理能力およびメモリ能力のために、スマートカードは従来のクレジットカードにとって代わり、代表的には、所定の口座から引き落としするカード保有者の権利を確認するために使用されることが期待されている。スマートカードは、スマートカードの所持者が正当な保有者であることの高水準の保証を提供する。これは、従来のクレジットカードの主要な問題を解決する。さらに、スマートカードは、口座から引き落とす（口座に振り込む）ための「許可証」以上のものとなる。例えば、スマートカードは、事前に承認されたクレジットを「運ぶ」ことができる。
【０００３】スマートカードが約束を果たすことを可能にするには、スマートカード内のコンピュータが不正用途に使用し得ないことが確実であるとサービス提供者が感じなければならない。この必要を満たすためにいくつかの方法が既に使用されている。第１に、スマートカードには、電源ポートと単一の情報通過ポートが備えられる。第２に、スマートカードに埋め込まれたコンピュータは、コンピュータに送られる命令がカードの目的およびセキュリティ指針に対して有害な動作を実行しないことを保証するオペレーティングシステムの制御下で動作する。すなわち、許容されたデータ領域を読み出す命令および変更する命令のみが可能である。第３に、今日のスマートカードの発行者は、リモート通信を通じてではなく、提供者の構内でカードを使用することを主張している。
【０００４】
【発明が解決しようとする課題】現在のスマートカード

のメモリは、複数のサービス提供者のプログラムおよびデータを保持するのに十分な大きさである。すなわち、単一のスマートカード上に、例えば、ビザ、アメリカン・エクスプレス、およびマスターカードが共存するのに十分な大きさのメモリがある。しかし、商業的な意味では、複数のサービス提供者のサービスをのせることに成功したスマートカードはまだ開発されていない。この状況は、いくつかのセキュリティ問題が解決していないためであると考えられる。例えば、だれがカードの所有者であるか、および、スマートカードのメモリ内のすべてのファイルに対して所有者はどのような権限を有するかに関して問題が生じる。商業的に言えば、他のサービス提供者が求めるセキュリティに一致しないスマートカードには、スマートカードの所有者（これもサービス提供者であることもある）はどの程度の権限を有するかという問題である。これは信用の問題である。
【０００５】第２の問題点は、リモート発給に関するものである。特に、カードを提供者のところに持って行くことによってのみサービスがインストールされるようにすることをスマートカード保有者に要求することは望ましくない。また、スマートカード上のサービスのうちの１つがキャンセルされるときにスマートカードの引き渡しを要求することも望ましくない。むしろ、商業的成功のためには、リモート発給を可能にすることが望ましく、おそらく本質的でさえある。
【０００６】リモート発給の問題点が解決すると、第３の問題点は、旧サービスがキャンセルされ新サービスがインストールされる際に保有者のスマートカード内の空間を再使用する必要に関するものである。
【０００７】第４の問題点は、競合サービス間の商業的衝突と、顧客が競合サービスにアクセスすることを制限するよう提供者が所望することである。
【０００９】
【課題を解決するための手段】上記の問題点は、サービス提供者またはスマートカードの所有者が、事前に許可なく、既存の各サービス提供者のためにまたは既存の各サービス提供者によって作成されたファイルにアクセスすることなく、異なるサービス提供者がスマートカード上で共存することを可能にするオペレーティングシステムによって解決される。
【００１０】スマートカードのオペレーティングシステムは、ＵＮＩＸ（ＵＮＩＸシステム・ラボラトリーズの登録商標）にやや似ており、スマートカードの発行者／所有者によって所有されるルートディレクトリを有し、各サービス提供者は発行者／所有者によってインストールされる「ユーザ」である。このような各ユーザには、ルートディレクトリのサブディレクトリが与えられ、そのサブディレクトリ内にユーザはファイルおよびファイルを含むサブディレクトリを、ユーザが必要とするだけ作成する。

5

【００１１】オペレーティングシステムは、スマートカードの発行者／所有者およびスマートカードの保有者を含むスマートカードの全ユーザに対して、ユーザが、所有するファイルに他のユーザからアクセスできないようにすることを選択した場合に、そのようなアクセスができないようにする。この排他能力は、ユーザによって所有され、スマートカードの発行者／所有者を含む他のユーザは変更できないパスワードファイルによって実現される。オプションとして、スマートカードの発行者／所有者には、与えられたユーザのすべてのファイルを消去する能力が与えられる。

【００１２】また、オペレーティングシステムは、ディジタル署名つき通信手段と、完全暗号化通信手段とを有する。この機能は、リモート通信における信頼性を与える。リモート通信により、リモート発給と、各スマートカードに含まれるすべてのサービスを追跡するデータベースの効果的な保守と、スマートカードの紛失または一般的故障の場合のスマートカードの再発給とが可能となる。

【００１３】

【実施例】いくつかのスマートカードオペレーティングシステムが既に知られている。１つの例は、米国特許第４，８１６，６５３号（発明者：アンダール(Anderl)他、発行日：１９８９年３月２８日）に記載されている。以下で説明するオペレーティングシステムは、そのオペレーティングシステムおよび周知のＵＮＩＸオペレーティングシステムと多くの類似点を有する。ここで説明するスマートカードオペレーティングシステムの理解を助けるため、ＵＮＩＸオペレーティングシステムのいくつかの周知の事項を簡単に説明しておく。

【００１４】［ＵＮＩＸオペレーティングシステム］ＵＮＩＸオペレーティングシステムはファイルの集合からなる。ファイルのうちのいくつかは、関連するファイルに関する情報を主に含み、ディレクトリファイルまたはディレクトリと呼ばれる。他のファイルはユーザデータを含み、「通常」ファイルという。また、ＵＮＩＸオペレーティングシステムでは、ユーザは、ファイルの「ｏｗｎｅｒ（所有者）」であるか、ファイルによって認識される指定された「ｇｒｏｕｐ（グループ）」に属するか、または、「ｏｔｈｅｒ」に属することができる。各ファイルは、所有権、３種類のユーザに関する情報アクセス能力などのようなファイル特徴を指定するデータ部分を含む。ファイルの所有者はすべてのファイル特徴を変更することができる。

【００１５】構造的には、最初のファイルはルートディレクトリファイルである。このディレクトリの所有者であるユーザは、実際、オペレーティングシステム全体の所有者である。このユーザはルートファイルによって指される他のファイルを作成することができる。そのファイルは、他の「ディレクトリ」ファイルであることも

6

「通常」ファイルであることも可能であり、ツリー上構造においてルートディレクトリの「下」にあるとみなされる。

【００１６】多くのＵＮＩＸオペレーティングシステムでは、ルートの下のディレクトリのうちの１つは「ｅｔｃ」と命名され、このディレクトリはその下に「ｐａｓｓｗｄ」というファイルを有する。このファイルの全アドレスすなわちパス名は「／ｅｔｃ／ｐａｓｓｗｄ」である（パス名の最初のファイル「／」はルートアドレスを表す）。「ｅｔｃ」および「ｐａｓｓｗｄ」ファイルは、一般にルートと呼ばれルートディレクトリの所有者でもあるシステム管理者によって所有される。「ｐａｓｓｗｄ」ファイルはルートのパスワードの暗号化表現を含み、オペレーティングシステムへのルートのアクセスはルートがパスワードを提示することによってログインした後でのみ許される。提示されるパスワードは暗号化され、「ｐａｓｓｗｄ」ファイルに格納された暗号化パスワードと比較される。比較が成功した場合、ユーザは認められ、他のファイルへのアクセスを許可される。すなわち、このユーザは「ログイン」したことになる。

【００１７】ルートが、ルートディレクトリの下にサブディレクトリを作成し、そのサブディレクトリの所有権を他のユーザに割り当てることにより、マルチユーザ機能を実現することができる。次に、ルートは、「ｐａｓｓｗｄ」ファイル内にそのユーザのパスワードをインストールし、そのユーザがそのパスワードを提示したときにそのサブディレクトリファイルにおいてシステムに入ることを可能にする。このユーザは自己のパスワードを変更する能力を有するが、それはオペレーティングシステムによって提供されるコマンドを通じてのみ可能である。そのパスワードは、システムにおいて、暗号化された形式でのみ、かつ、「ｐａｓｓｗｄ」ファイル内にのみ存在する。このアーキテクチャを図１に示す。

【００１８】ログインプロセスは次のように要約することができる。ＵＮＩＸオペレーティングシステムのもとで動作するコンピュータは、コンピュータの入力ポートをスキャンするループを実行することによって始動する。ユーザによる接続が検出されると、制御は、そのループからそのユーザとの対話を開始したプログラムに移る。そのプログラムは「ｌｏｇｉｎ：」メッセージをユーザに送り、ユーザの応答を待つ。ユーザが、例えばストリング「ｈｔｂ」を返すことによって、自己を表示し、これが、そのユーザをオペレーティングシステムに対して識別させる。次に、プログラムは、要求メッセージ「Ｐａｓｓｗｏｒｄ：」を出し、ユーザはパスワードストリングを提示しなければならない。プログラムはそのパスワードストリングを暗号化し、それを、「／ｅｔｃ／ｐａｓｓｗｄ」ファイル内にあるその識別したユーザの暗号化パスワードと比較する。一致した場合、ユーザは真正であると判定され、制御はルートによって所有

されるファイル（代表的には、「．ｐｒｏｆｉｌｅ」と命名されている）に渡される。このファイルはそのユーザに対してさまざまなパラメータを設定し、制御を、ユーザによって所有されるもう１つのファイル（代表的にはこれも「．ｐｒｏｆｉｌｅ」と命名されるが、このファイルはそのユーザによって所有されるディレクトリ内にある）に渡される。そのユーザの「．ｐｒｏｆｉｌｅ」内にある命令が実行された後、コンピュータはループに入り、ユーザからの次の命令を待つ。

【００１９】ルートは、「ｐａｓｓｗｄ」ファイルを含めて、オペレーティングシステムを構成するすべてのファイルの所有者である。従って、ルートは、任意のファイルを変更することが可能であり、従って「スーパーユーザ」である。ルートによって所有されていないファイルであっても、ルートのコマンドに従うことが重要である。それは、ルートが、「ｐａｓｓｗｄ」ファイルとともに、ルートの能力を制御するファイルをも一般的に変更する能力を有するためである。この能力によって、ルートはパスワードを変更する能力を有し、従って、ルートは常にファイルの所有者になることができる。従って、ルートに所有者のすべての能力を直接持たせることは意味がある。簡潔に言えば、ルートは、システム内のすべてのファイルの絶対的制御および全情報を有する。

【００２０】（正確なパスワードを提示することによって）ログインすることができることに加えて、ユーザには、ファイルの読み出し、ファイルへの書き込み、ファイルの実行（すなわち、プログラム制御をファイルに渡すこと）の能力が与えられる。（指定したファイルにプログラム制御を渡す能力がなければ、何も行うことができない。）プログラムを実行することは、制御をファイルに渡すことにほかならないからである。ルートはシステムのすべてのファイルにアクセスすることができるため、ルートはすべてのファイルを読み出し、書き込み、実行することができる。

【００２１】ＵＮＩＸオペレーティングシステムのすべてのシステム提供の命令は、単に実行可能なファイルであり、これらのファイルは、そのファイルがどこにあるかをシステムが知っている限り、どのディレクトリにも存在することができる。既に述べたように、ルートはそのようなすべてのディレクトリおよびファイルを所有する。ルートはそれらのすべてのディレクトリおよびファイルの読み出しおよび実行の許可を制御するため、ルートは、単にファイルの許可（パーミション）を制限することによって、任意のユーザ（必要な場合には、自分自身を含めて）が、任意のファイルを実行しないように制限することが可能である。これにより、ルートは、ユーザの特定のグループによる実行が制限されたファイルのカスタム化したセットを作成することができる。換言すれば、ルートは、システムで利用可能なすべてのコマンドより少ないコマンドを含む、さまざまな制限されたオペレーティングシステム、すなわち、「制限シェル」を作成することができる。

【００２２】［スマートカードオペレーティングシステム］ＵＮＩＸオペレーティングシステムでルートが有する絶対的な能力は、スマートカードには不適当である。明らかに、ビザ、マスターカード、およびアメリカン・エクスプレスのような提供者は相互にルートであることを許容しないであろうが、明白に十分なセキュリティ手段がなければ、それら以外の第三者がルートとなることも望まないと考えられる。これは、スマートカードが、受けるべき商業的成功を収めない問題点の一部である。

【００２３】図２に、このサービス提供者の敏感さに対応する構造を示す。図２の構造によれば、ルートは、ルートディレクトリおよび作成したい任意の数のファイル（ディレクトリファイルまたは通常ファイル）を所有する。例えば、図２は、ルートディレクトリファイル１０を含み、その下には、「．ｐｒｏｆｉｌｅ」ファイル１１、「ｐａｓｓｗｄ」ファイル１２、「ｌｏｇ」ファイル１７、「ｆｉｌｅｘ」ファイル１３、「ｆｉｌｅｙ」ファイル１４、および「ＩＤ」ファイル１８がある。ルートの下にはいくつかのサブディレクトリも存在し、それぞれユーザ（サービス提供者）の「ＨＯＭＥ」ディレクトリとして使用される。例えば、図２は、「ｈｔｂ」という名前（スマートカードの保有者）のディレクトリファイル１５、「ｂａｎｋＡ」という名前のディレクトリファイル２０、および、「ａｉｒｌｉｎｅＡ」という名前のディレクトリファイル２５を含む。各ディレクトリは、対応するユーザのＨＯＭＥディレクトリの下に、「ｐａｓｓｗｄ」ファイル（それぞれ１６、２１、および２６）と、「．ｐｒｏｆｉｌｅ」ファイルを含む。パスワードファイルのこの配置はいくつかの利点を有するが、これは必須ではない。重要なことは、このような各パスワードファイルの所有権はそのファイルおよびそのうえのディレクトリに対応するユーザに割り当てられることである。ディレクトリ１５、２０および２５の所有権を各ユーザに与えることも有益である。

【００２４】図２は、もう１つの重要なディレクトリ（およびユーザ）を含む。それは、「Ｖｉｓｉｔｏｒ」ディレクトリ３０であり、これは、スマートカードと対話したい非サービス提供者のエントリポイントである。

【００２５】図２のファイルアーキテクチャは、ＵＮＩＸオペレーティングシステムとは異なるオペレーティングシステムと結合される。図２の構造のオペレーティングシステムは、主に、そのオペレーティングシステムではルートが所有しないファイルを変更する能力がルートには与えられないという点でＵＮＩＸオペレーティングシステムとは異なる。この機能がルートによって迂回されないことを保証するために、このオペレーティングシステムでは、ルートが、オペレーティングシステムを定義するいくつかのファイルを変更することを許容しない

9

（ある意味では、ルートはそれらのファイルを所有しない）。この結果を実現する１つの手段は、それらの非ルート所有オペレーティングシステムファイルを読み出し専用メモリ（ＲＯＭ）に格納することである。少なくとも、このＲＯＭは、ファイルへの書き込みを行うコマンド／モジュール／ファイルを含む。特に、ファイルへの書き込みは、ファイルの所有者が指定したものに制限され（ファイルの所有者は、最初は、そのファイルを作成したユーザである）、ルートは単に他のユーザとして扱われる。ファイルへの書き込みを行うコマンドは、例えば、ファイルの移動、ファイルのコピー、ファイルの保存、ファイル属性（例えば所有権）の変更、およびファイル名の変更のようなオペレーティングシステムコマンドである。（各スマートカードに固有であるため）ＲＯＭ（さらに一般的には「一回書き込み」メモリ）にインストールされる他の事項は、ルートパスワードおよびスマートカードのＩＤ情報（すなわち、ファイル１２および１８）である。ＩＤ情報は、単に任意のストリングであることも、保有者の名前を含むことも可能である。保有者の名前を含むことは、おそらくは、ＩＤ情報を得た商人には望ましい。実際には、ルートパスワードおよびスマートカードのＩＤはいずれもルートディレクトリ（すなわち、ブロック１０）を構成するファイルに格納することが可能である。図２では、説明のために、これらは独立のファイルとなっている。

【００２６】いくつかの実施例では、１つのファイル書き込み能力がルートに与えられ、これは、任意のファイルを全体として削除する能力である（そして、そのプロセスで、実質的には、削除されたファイルが指しているファイルを削除する）。これには、ディレクトリファイルおよび通常ファイルが含まれ、ルートが所有するファイルにもルートが所有しないファイルにも適用される。このような能力は、与えられたサービス提供者がスマートカードの保有者にもはやサービスを提供していないときにメモリ空間が再使用されるような実施例で与えられることが可能である。

【００２７】図２のオペレーティングシステムと標準的なＵＮＩＸオペレーティングシステムのもう１つの相違点は、前者が、ルートによって所有されるファイルに（例えば「ｆｉｌｅｘ」１３に）インストールされた暗号キー対を含み、このキー対は各スマートカードに固有であるという点である。この対は、スマートカードによって秘密に保持される私的キーｆと、スマートカードが秘密に保持するようには注意しない公開キーｇとを含む。もちろん、両方のキーは、スマートカードのルートユーザ（すなわち、スーパーユーザ）でもあるスマートカードの所有者／発行者には最初から既知であるが、ルートは私的キーを保持する必要はない（そしておそらくその情報を破壊することを選択することになる）。このキー対はルートのパスワードを含むメモリのような適当

10

なメモリに「焼き付けられ」、または、ルートディレクトリを定義するファイルに含められることも可能である。公開キー暗号化については後でさらに詳細に説明する。

【００２８】ユーザのディレクトリのパスワードがそのユーザによって所有されるファイルに格納されるということは、ＵＮＩＸオペレーティングシステムと図２のオペレーティングシステムの重要な相違点である。これらのパスワードをそのファイルの所有者以外の者が読み出すことができないということは、そのパスワードを暗号化しない形式で格納することを可能にする。書き込みに対する制限とともにこの構成によって、ルートは任意のファイル（通常ファイルまたはディレクトリファイル）の所有者になることはできなくなり、従って、ルートはファイルの所有者によって設定された許可を迂回することができなくなる。この重要な相違点によって、あるユーザのファイルは、ルートおよび他のユーザに対して完全に不透明となる。このようにして、図２の構成は、サービスの提供者とスマートカードの発行者／所有者の間の「信頼問題」を克服する。

【００２９】［取引セキュリティ］解決すべき次の問題はスマートカードの取引セキュリティである。この概念は、スマートカードの保有者またはサービス提供者に悪影響を及ぼすような無許可の取引が起こらないことを保証するために、スマートカードのオペレーティングシステムによって、および、通信プロトコルに同意した者によって、使用される手段を含む。これは、ルート、保有者、サービス提供者、ビジター（Ｖｉｓｉｔｏｒ）ユーザ、または侵入者による活動を含む。（侵入者とは、スマートカードと他者の間の通信セションに介入し、自己のメッセージを真のメッセージと置き換える者のことである。）

【００３０】侵入者に対抗する１つの方法は、日付および時刻のタイムスタンプを含むメッセージを構成し、メッセージの少なくともその部分を暗号化することである。また、必要な場合には、通信プロトコルが、確認シーケンス（これはセションごとに異なる）を当事者間で交換することを要求することも可能である。また、パスワードのような微妙な情報の明文でのフローを最小にするのも有効な一般的方法である。これらの技術は、後述のログインおよび通信プロトコルで使用される。

【００３１】［暗号化］暗号化の分野は新しくない。以下の説明は、単に、本発明のスマートカードに関連して使用可能な２つの暗号化方式の要約である。

【００３２】周知のように、暗号化のための「秘密共有」方式は、２つの通信者が秘密の関数ｆを共有することを要求する。メッセージｍを送信したいほうの側は、その秘密関数でそのメッセージを暗号化して暗号化メッセージｆ（ｍ）を形成する。この暗号化メッセージは送信され、受信側は関数ｆ（ｆ（ｍ））を形成することに

よって受信した信号を復号する。関数ｆは、ｆ（ｍ）からメッセージｍを発見することが計算量的に非常に困難であるが、その関数を２回適用することによってもとのメッセージが復元されるような関数（すなわち、ｆ（ｆ（ｍ））＝ｍ）である。

【００３３】暗号化のための「秘密共有」方式は非常に有効であるが、その弱点は、秘密関数を通信する（すなわち、共有する）必要があることである。その関数が伝送されているときの稀な通信セション中にその共有の秘密が傍受者によって取得されてしまうと、もはやそれは秘密ではなくなる。

【００３４】公開キー暗号化では、各当事者はキーの対ｆおよびｇのうちの一方を保持する。特に、一方の当事者が一方のキー（ｆ）を秘密に保持し、それを通信することはないが、他方のキー（ｇ）は、すべての者に知らせる。従って、キーｇは「公開され」、キーｆは「私的」である。対ｆおよびｇは次の３条件を満たすようなものである。

１．ｇ（ｆ（ｍ））＝ｍ。

２．ｇが既知である場合でも関数ｆは決定することができない。

３．ｆ（ｍ）からメッセージｍを決定することは計算量的に実現不可能である。

【００３５】公開キー方式は、前述のキー分配／管理の問題を解決するが、この方法は１つの欠点を有する。それは、公開キーの暗号化および復号が共有キー方式よりも遅い（より多くの計算時間を必要とする）ということである。

【００３６】スマートカードに関しては、通信速度は、スマートカードと通信している当事者の種類に基づいて、異なる重要度を有する。スマートカードの発行者／所有者およびサービス提供者に関しては、通信は稀であることが予想され、従って、処理時間は「最重要」ではないため、低速度は主要な欠点ではない。しかし、それ以外の者（すなわち、ビジターユーザとしてログインする商人）との通信では、速度は重要である。

【００３７】速度の問題は、必要であれば、「共有秘密」方式を公開キー方式と組み合わせることによって解決される。すなわち、通信を開始するとき、公開キー方式を使用して一時的な「共有秘密」をスマートカードと商人の間で通信する。特に、公開キーを有する側は「共有秘密」を提示し、それを、私的キーを有する側へ通信する。その後、より高速に、「共有秘密」方式を使用して全メッセージを暗号化する。

【００３８】あるいは、（共有秘密を用いて）認証方式を使用することも可能である。認証方式では、メッセージは明文で送信され、「ディジタル署名」が追加される（すなわち、「署名される」）。「ディジタル署名」は、符号化されるメッセージのハッシング（例えば、ある数を法としての、メッセージ内の文字のＡＳＣＩＩコードの加算）である。もちろん、侵入者が真のデータを偽データで置き換えることができないことが保証されるようなアプリケーションでは、（おそらくは、公開キーを使用した確認プロセスの後で）情報は明文で送ることができる。

【００３９】公開キー方式の使用は、キー管理のほとんどの問題を解決する。スマートカードと通信したい当事者の公開キーの初期情報の問題がなお残るが、スマートカード自体がその情報を提供することができるので、それは問題ではない。

【００４０】［ルートによるログインおよびサービス提供者／ユーザのインストール］暗号化が安全な通信を保証するため、スマートカードの発行者／所有者はサービスのリモートインストールを信頼することができる。もちろん、発行者／所有者（すなわち、ルート）は、最初に、スマートカードにログインしなければならない。ログインのためのプロトコルを図３に示す。また、サービスインストールプロセスのためのプロトコルを図４に示す。本発明のスマートカードとの間で可能な物理的にリモートの接続を図８に示す。

【００４１】図３に示したように、プロセスは、スマートカードの所持者（Ｐ）がスマートカード（Ｓ）の真正な保有者として認証されることから開始する。図３に示したように、プロセスは、スマートカードからのプロンプトと、スマートカードに所持者のＰＩＮ（個人識別番号）を入力することによって開始する。所持者を認証するためにスマートカードの処理能力を使用することは、ＰＩＮを捕捉する可能性のある装置にＰＩＮストリングを通信する必要がないという点で有利である。ＰおよびＳが商人の構内に存在するようなアプリケーションであっても、商人の装置は、安全にスマートカードとインタフェースするスタンドアローン型の装置とすることが可能である。この装置は、電池で動作し、キーボードおよびディスプレイを有し、他のポート、プロセッサ、および書き込み可能メモリを有しないことが確認することができる。動作時に、ＰはＳをこのスタンドアローン装置に挿入し、キーボードでＰＩＮを入力し、スマートカードはそのＰＩＮが正しいかどうかを判定する。正しければその装置のディスプレイはメッセージ「ＯＫ」を出力する。このようなスタンドアローン装置が利用可能でない場合（または、例えば所持者の家庭で「ダム」カードリーダを使用するときのように通信がリモートである場合）、提示されるＰＩＮはスマートカード内で処理されるべきであり、スマートカードからの（商人の装置への）「ＯＫ」メッセージは「タイムスタンプ」され、暗号化される。このことは、適当な暗号化キーが確立され日付および時刻の情報がＳに伝えられた後まで、ＰがＨとして確認されることは延期されなければならないことを示唆する（これは図３に示した方法ではない）。

【００４２】図３に戻って、一般に、Ｈの真正な地位が

確立された後、Ｓは、ログイン中のユーザが正当なユーザであることを確認し、ユーザは、Ｓが正当なスマートカードであることを確認する。特に、図３のプロトコルは、全体として、次のように進行する。

【００４３】ａ．Ｓは入力を促し、ＰはＰＩＮストリングを提示する。スマートカード内では、ＰＩＮは、保有者が変更するためにオープンされたルート所有のファイル（例えば、図２のファイル１４）内に存在する。Ｓは、提示されたＰＩＮストリングを、格納されているＰＩＮストリングと比較し、一致すれば、ＰはＨとして確認されたことになる。

【００４４】ｂ．Ｈが確認されると、ＳとＯの間の通信に注意を向けることができる。Ｓは、そのＩＤ番号と、ランダムストリングの形式でのパスワードチャレンジＲＮＤ１とをＯに提示することによって自己を表示する。

【００４５】ｃ．ＯはＯのパスワードでＲＮＤ１を暗号化してストリングK_1（ＲＮＤ１）を形成し、それをＳに返す。このパスワード応答の形式は明白にセションごとに変化し、Ｏの真のパスワードが侵入者によって盗まれないことを保証する。Ｏが所有するすべてのスマートカードのパスワードをどこに保持し、このようなデータベースはどのくらい安全かという問題が残っている。しかし、実際にはＯはパスワードのデータベースを保持する必要はない。Ｏに必要なのは、Ｓによって供給されるデータとともに処理するとスマートカードのパスワードとなる単一のシードのみである。そのデータはＩＤ情報である。

【００４６】ｄ．スマートカードによって提示されるストリングは、常に、同一であるか、Ｏには事前には未知であるかのいずれかであるため、初期ストリング（ＩＤ，ＲＮＤ１）が記録の再生でないことを保証するために追加の認証ステップが所望されることもある。これは、Ｏが、例えば、そのＩＤとランダムストリングとからなるチャレンジメッセージＲＮＤ２をＳに送ることによって実現される。

【００４７】ｅ．ＲＮＤ２ストリングに含まれるＩＤに基づいて、Ｓは、Ｏがユーザであると判定し、必要なキー（例えば、Ｏのパスワード）を取得し、K_1（ＲＮＤ１）を復号する。復号の結果ＲＮＤ１となると、Ｓは、Ｏが真正であると判定する。

【００４８】ｆ．その後、ＳはＳのルートパスワードでストリングＲＮＤ２を暗号化し、その結果のストリングK_1（ＲＮＤ２）をＯへ転送する。

【００４９】ｇ．ＯはK_1（ＲＮＤ２）応答を復号し、その結果のストリングがＲＮＤ２である場合、ＯはＳが正当であることに満足する。これでログインプロセスは終了し、ＯはＳにプロンプトを提示し、サービスの要求を受ける準備ができた状態になる。

【００５０】上記の「ログイン」プロセスは、アクセスしたいコンピュータが制御するような周知のログインプロセスとは異なるように見えることに気づくかもしれない。コンピュータはユーザの初期識別情報を要求し、次にパスワードを要求する。その初期識別情報に基づいて、コンピュータはどのパスワードが期待されるかを知る。一方、スマートカードは、（Ｏとの）通信を開始するという意味では制御されているように見える。しかし、初期識別情報を要求する（情報を得る）代わりに、スマートカードは、情報すなわちＩＤおよびＲＮＤ１を提供する。これは、Ｏからの応答が初期識別情報なのか、それとも、パスワードなのかという問題を引き起こす。これがパスワードであれば、Ｓはそのパスワードが正しいか否かをどのようにして知るのであろうか。その答えは、Ｏからの応答が３つの目的のために使用されるということである。Ｏは、（ＲＮＤ１に含まれるＩＤによって）初期識別情報の意味で自己を表示し、ＲＮＤ１を暗号化するために正しいキーを使用することによって自己を認証し、暗号化モードで返されるＲＮＤ２によってＳの正当性を問う。

【００５１】Ｏがログインされると、Ｈは、サービス提供者（ＳＰ）によって提供されるサービスのインストールの要求を通信することができる。Ｏによってインストールされるよう要求された特定のサービスに関する通信は、人間との対話を含むこともあるが、自動化も可能である。例えば、Ｈは、所望されるサービスをＳに通信し、ＳがＯと通信することが可能である。図４に、サービスのインストールのためのプロトコルを示す。

【００５２】ａ．Ｈはサービス要求をＳに転送する。

【００５３】ｂ．Ｓはこの要求を暗号化し、それをＯへ転送する。ＯとＳの間の電子通信は、Ｓ内の公開キーの私的キー要素で暗号化可能である。Ｓはその公開キーをＯに送っておく。あるいは、通信は、スマートカードの「共有秘密」でも暗号化可能である。「共有秘密」としてルートパスワードを選択することが可能であり、または、一時的な「共有秘密」を（上記のように、公開キー暗号化を使用して）ＯからＳへ提供することが可能である。図４では、ルートパスワードを暗号化に使用して、要求ストリングK_1（ＲＥＱ）を作成している。

【００５４】ｃ．要求されたサービスを知ると、ＯはＳＰと交信し、ＳＰがサービスをＨに提供することに同意することを確認する。

【００５５】ｄ．サービスの提供がＳＰに同意されると、Ｏは一時的パスワードを選択し、そのパスワードをＳＰに（おそらくは暗号化通信によって）通知してから、Ｓ内にＳＰのためのディレクトリおよびパスワードファイルを作成する。

【００５６】ｅ．パスワードファイルがＳＰユーザのために設定されると、その一時的パスワードがＳに（上記のように、暗号化通信によって）送られ、このディレクトリおよびパスワードファイルの所有権はＳＰに移転される（このパスワードは、将来のＳＰとの通信セション

において「共有秘密」キーとして利用可能である）。また、ＳＰが必要とするその他のアプリケーションソフトウェアはこのときにインストールすることが可能であり、Ｏがそれらのファイルを暗号化モードで送信する。あるいは、アプリケーションソフトウェアはＯによってインストールされないようにも設定可能である。

【００５７】ｆ．この時点でＨには、最終セットアップのためにＳＰと交信するよう通知される。

【００５８】ｇ．Ｈは、図３のようなログインシーケンスを使用して、ただし、暗号化キーとして一時的ＳＰパスワードを使用して、ＳとＳＰの間の通信路を設定する。

【００５９】ｈ．ＳＰへのログインが確立すると、Ｓはサービス要求を送出し、ＳＰは応答して、新しいパスワードと、Ｏによってインストールされなかった必要なファイルと、データとをインストールする。これでサービスインストールプロセスは完了する。

【００６０】［サービス提供者によるサービスの提供］上記のように、サービス提供者は、単に、スマートカードに割り当てられたディレクトリを有するユーザである。サービス提供者は、プロセッサがスマートカードとサービス提供者の間の通信を確立するとログインする。前のように、ログインプロトコルには３つの要素がある。

（１）ＳＰは、ＰがＨであることを確定したい。

（２）Ｓは、ログインするユーザが真のＳＰであることを判定したい。

（３）ＳＰは、正当なＳと通信していることを判定したい。

【００６１】これらの３つの要素は、図３について説明したプロトコルで実行される。ログイン成功後にのみ、サービス要求を進めることができる。サービス要求は、例えば、ＨがＳＰ（例えば銀行）に、Ｓの「電子財布」を満たすことにより、Ｓに「お金」をインストールすることを要求することである。電子財布の充填とは、例えば、単に、ＳＰによって所有されるあるファイルにある値をインストールすることである。これは図５の流れ図に示されている。

【００６２】［商人との対話］十分ゆとりがある場合、スマートカード保有者は、スマートカードとビジター（Ｖ）ユーザである商人とを対話させたいと思うことが予想される。上記の方式によれば、このような対話は２つの方法で可能である。１つは、スマートカードと商人との直接対話であり、もう１つは、スマートカード、商人、およびサービス提供者を含む三者間対話である。三者間対話方式のためのプロトコルは、図６に示すとおりであり、以下のようになる。

【００６３】ａ．ＰはＳとＶの間に（ＳをＶに渡すことによって、または、ＳをＶにリモート接続することによって）通信を確立する。

【００６４】ｂ．Ｓは入力を促し、ＰはＰＩＮストリングを提示する。これが正しく一致すれば、Ｓは、ＰがＨであると判定し、標準の「ログイン」シーケンスに進み、そのＩＤ情報およびＲＮＤ１を送る。

【００６５】ｃ．ＶはＳＰとの通信路を設定し、ＳＰに自己を表示し、ＩＤ情報およびＲＮＤ１を中継する。

【００６６】ｄ．ＩＤ情報が与えられると、ＳＰはそのパスワードを（おそらくは、処理とともにシードストリングも使用して）決定し、そのパスワードでＲＮＤ１を暗号化する。その結果のストリングK_2（ＲＮＤ１）が、ランダムストリングＲＮＤ２とともにＳに送られる。

【００６７】ｅ．Ｓは、ＳＰがK_2（ＲＮＤ１）を形成する際に正しいパスワードを使用したかどうかを判定し、その結論が真であれば、ＲＮＤ２を暗号化し、その結果K_2（ＲＮＤ２）をＳＰに転送する。

【００６８】ｆ．ＳＰは、Ｓが正しいパスワードを使用してＲＮＤ２を暗号化したことを確認すると、プロンプトをＶに送り、商人に、Ｓの使用の要求に進むことができることを通知する。

【００６９】ｇ．ＶはＳＰからのアクション（例えば、ＳＰにあるＨの口座からある値を削除する、または、ＳにありＳＰによって所有されるファイルのある値を変更する）を要求する。

【００７０】ｈ．ＳＰはその要求を満たし、必要であれば、ＳＰパスワードで暗号化した適当なコマンドをＳに送る。

【００７１】スマートカードに商人（または、商人の銀行、もしくは、商人にサービスを提供し商人の代わりをする者と提携した商人）と直接対話させたい場合、スマートカードと事前に確立した関係を有しない者がスマートカードにログインすることを可能にするメカニズムを確立する必要がある。「ビジター」ユーザディレクトリがこの要求を満たし、このユーザはパスワードを有しない。結果として、ビジターユーザは非常にセキュリティのないユーザであるため、Ｖのアクセスは厳格に制御されなければならない。

【００７２】例えば、解く必要のある１つの問題は、このようなビジターユーザが、商人によって指定されるサービス提供者のみのアプリケーションファイル（プログラム）にアクセスすることができるのか、それとも、すべてのサービス提供者のアプリケーションファイルにアクセスすることができるのか、ということである。すべてのサービス提供者のアプリケーションファイルへのアクセスが許可される場合、最も簡単な方式は、ルートが、パスワードなしでビジターユーザディレクトリを設定し、ビジターユーザがオペレーティングシステムコマンドの制限されたセットのみを実行することを可能にする制限シェルを与えることである。すなわち、変数ＰＡＴＨを、ルートによって所有される１つのディレクトリ

17

（いくつかのオペレーティングシステムコマンドのみを含む）と、ＳＰがビジターユーザに実行アクセスを許可したい実行可能ファイルを含むＳＰサブディレクトリ（またはサービス提供者／ユーザの選択したサブディレクトリ）とを含むように設定する。

【００７３】指定したＳＰのみのアプリケーションファイルにアクセスを許可する場合は、もちろん、ＳＰを指定しなければならず、指定したＳＰの実行可能ファイルのみを含む手段を設けなければならない。この場合も、これは制限シェルによって容易に実現され、ＰＡＴＨ変数は指定したＳＰのディレクトリ（または選択したサブディレクトリ）を含む。プロトコルは、図７に示すとおりであり、次のようになる。

【００７４】ａ．Ｓは入力を促し、ＰはＰＩＮストリングを提示する。これが正しく一致すれば、Ｓは、ＰがＨであると判定し、標準の「ログイン」シーケンスに進み、そのＩＤ情報およびＲＮＤ１を送る。

【００７５】ｂ．Ｖは、パスワードを有しないため、単にストリングＲＮＤ１を返す。

【００７６】ｃ．この応答によって、Ｓは、ユーザがビジターユーザであることを認識し、公開キーK_{pu}を送出する。（公開キーは、ＩＤ情報の一部として既に送ってしまっていることも可能である。）この時点で、Ｓは、公開キー、ＩＤ情報およびＲＮＤ１を含むメッセージから導出される「ディジタル署名」を送ることもできる。また、Ｓは、提案する「共有秘密」（図７には図示せず）を構成する暗号化ストリングを送ることもできる。ディジタル署名は公開キーで暗号化される。

【００７７】ｄ．Ｖは、提供された公開キーを使用して「ディジタル署名」を解読する。解読した「ディジタル署名」が適当なストリングと一致した場合、ＶはＲＮＤ２を送出する。

【００７８】ｅ．Ｓは、公開キーでＲＮＤ２を暗号化し、K_{pr}（ＲＮＤ２）によって応答する。

【００７９】ｆ．Ｖは、このメッセージをK_{pu}で復号し、ＲＮＤ２を取得した場合、Ｓと通信していることを確定する。

【００８０】ｇ．Ｖは、時刻および日付の情報を、K_{pu}で暗号化してＳに送り、Ｓはプロンプトを返す。

【００８１】ｈ．Ｖは、同じくK_{pu}で暗号化して要求（Ｖが求めるアクションおよび使用されるＳＰを識別する）をＳに送信し、Ｓは、指定されたＳＰと交信する許可によって応答する。この許可は、公開キーK_{pr}で暗号化される。

【００８２】一般的に、商人は、商人によって提供される商品またはサービスと引き換えに、Ｈに属する資金を得たいと考える。上記のように、銀行のようなサービス提供者が、ある値を保持する「電子財布」をインストールすることは全く可能である。この値は、サービス提供者によって所有されるあるファイル内にある。

18

【００８３】商人は、このファイルにアクセスしたいと考え、ＳＰ（Ｈと提携している）はこのファイルへのアクセスを許可するが、その許可は非常に制限され厳格に制御されてのみなされる。このように、ＳＰは、オペレーティングシステムによって期待される規定の名前で、あるファイルを作成し、そのファイルに、ある値および特定のオペレーティングシステムコマンド（これはルートによって所有されない）を入れ、そのファイルにアクセスし、そのファイル内のその値から金額を差し引く。

【００８４】そのようなコマンドの流れ図を図９に示す。ブロック２００で、コマンドは、ビジターユーザディレクトリ内の（規定された名前の）ファイルを参照することにより開始する。このファイルは、例えば改行文字によって区切られた４個のエントリを含まなければならず、オペレーティングシステムは、この４個のエントリが、ａ）日付および時刻と、ｂ）商人のＩＤ（例えば、名前、住所、およびおそらくはコード）と、ｃ）差し引く金額と、ｄ）使用する「電子財布」を有するサービス提供者とからなると仮定する。

【００８６】このファイルが存在しない場合、または、要求された数のエントリを有しない場合、制御はブロック２１０に移り、商人（ビジターユーザ）にこの不足を通知する。ファイルが存在する場合、ブロック２２０で、コマンドは、サービス提供者（ＳＰ）の「電子財布」ファイル内の値を読み出す。ブロック２３０は、商人が引き出したい金額が電子財布内の値より大きいかどうか評価する。金額のほうが大きい場合、制御はブロック２４０に移り、拒絶メッセージを構成しそれを商人に、および、スマートカード内のログファイルに転送する。金額が値より低い場合、制御はブロック２５０に移り、ログファイルで、さまざまな不正の兆候がないかどうか検査する。これは、実行中のコマンドによって呼び出される別のコマンドとすることも可能である。図３に示すように、ブロック２５０は、３種類の出力を生じる可能性がある。第１は、潜在的不正条件（例えば、この商人は、事前に選択されている時間間隔内に規定の回数より多くスマートカードを使用した）を示唆する。第２は、ＳＰによって提供され商人にＳＰと取引について協議させるしきい値ファイルに応答する。第３は、標準状態を表示する。

【００８７】潜在的不正条件は、保有者のログファイルに格納されている情報によって処理され（ブロック２６０）、その後制御はブロック２４０に移る。格納されている情報は、商人、引き出そうとした額、拒絶理由などを識別する。これは、保有者に、カードの発行者／所有者と、および必要であれば政府当局と対話するのに必要な情報を提供する。必要に応じて、不正条件の疑いがあるときにスマートカードは無効にされる。

【００８８】ＳＰによって設定されたしきい値を超過した（例えば、ＳＰが、１０００ドルを超える引き出し許

可を「リアルタイムで」求めた）場合、ブロック２７０でメッセージが構成され、制御はブロック２８０に移る。

【００８９】ブロック２８０は、標準状態が示されたときにもブロック２５０から直接到達する。ブロック２８０は、スマートカードのログファイル内にあるシーケンス番号をインクリメントし、値ファイル内の金額から商人が要求する金額を差し引く。その後、ブロック２９０は、新しいシーケンス番号、日付および時刻、商人の識別情報、金額、およびＳＰからなるストリングを作成する。ブロック３００は、ストリングのディジタル署名を作成し、ブロック３１０は、ブロック２２０で構成されたメッセージと、ブロック３００で構成されたストリングと、ディジタル署名とからなるメッセージを作成する。最後に、このメッセージが、商人に、および、スマートカードのログファイルに送られる。

【００９０】商人の装置は２つのことのうちの１つを行う。ＳＰと協議するようにとのメッセージが存在する場合、商人の装置はＳＰに接続され、ブロック３１０で作成されたメッセージを転送する。その後、商人は、金額に対する即時クレジットを得ることができる（もちろん、署名に基づいて、そのメッセージが正当であると結論される限り）。商人によって受信されたメッセージがブロック２２０によって構成されたメッセージを含まない場合、商人は単に、許可ストリングを格納し、選択された時間間隔（例えば就業日全体）にわたりこのような許可ストリングを収集し、その後、その許可ストリングを適当なＳＰに転送する。

【００９１】許可ストリングはＳの公開キーで暗号化されているように示されているが、指定されたＳＰのパスワードで暗号化することも可能である。許可ストリングは、商人が単にそれを所定回数複製してＳＰに送ることがないことを保証するように十分強固でなければならない。これはいくつかの方法で実現することができる。それには、日付および時刻のタイムスタンプを有すること、値ファイル内の「前」および「後」の値の表示を有すること、Ｓによって供給されるシーケンス番号を有すること、などが含まれる。この許可ストリングはＶによって解読可能でなく、従って、変更不能であるため、セキュリティは保持される。

【００９２】［サービスセンタとしてのスマートカード発行者／所有者］本発明の１つの特徴は、スマートカードの発行者／所有者（Ｏ）が、スマートカード上に存在する「アプリケーション」を有するサービス提供者の一般的知識を有し、そのサービス提供者を制御することである。第１に、Ｏはサービス提供者のディレクトリの設定を制御する。第２に、Ｏは、保有者の要求に応じて、または、Ｏがスマートカードにアクセスすることができるときには、（保有者の同意の有無に関わらず）任意のディレクトリを削除することができる。第３に、Ｏはスマートカードを共有するすべてのサービス提供者の識別情報と、それらのサービス提供者のさまざまな詳細を知る唯一の当事者である。第４に、オペレーティングシステムの設計を通じて、Ｏは、各サービス提供者がアクセスすることができるメモリの量を制御し、従って、スマートカード上に「共存」することが可能なサービス提供者の数を制御することができる。第５に、Ｏは特定の種類の取引に対してサービス提供者のグループ化を定義することができる。第６に、Ｏは、サービス提供者によって占有される空間に比例して、スマートカード上に存在する権利に対してそのような各サービス提供者に課金することができる。

【００９３】上記のすべてのことから明らかなように、本発明の方式からいくつかの利益が生じる。前に述べていないことは、Ｏは、欠陥のあるカードを「修理」し、すべてのサービスを再インストールする能力を有する（所有者の代表的能力）。反対に、Ｏは、すべてのディレクトリを削除する能力を有し、この能力は、セキュリティ違反が起きたと判定されたときに執行される。

【００９４】セキュリティに関しては、考慮する必要のある４つの形式の攻撃がある。第１は、侵入者がルートになろうとする場合である。第２は、侵入者がサービス提供者になろうとする場合である。第３は、当事者（ルート、サービス提供者、侵入者、ビジター、保有者）が、許可されている以外のことをしようとする場合である。第４は、所持者が真正の保有者でない場合である。

【００９５】第１の形式の攻撃に関しては、最初の主要な関門はルートパスワードである。これは、ルートとしてのログインが試みられたが失敗したときにオペレーティングシステムがスマートカードを完全に無効にするように設定されるという意味で有効な関門である。例えば、すべてのディレクトリを消去することができる。

【００９６】サービス提供者としてログインしようと試みることは、わずかにゆるい方法でのみ扱われるべきである。すなわち、カウンタが、サービス提供者としてログインしようとして失敗した試行を追跡するように設定することが可能である。試行失敗回数が事前に選択した値（例えば４）を超えた場合には、スマートカードは無効になる。このような状況では、スマートカードの無効を、攻撃の対象であったサービス提供者のディレクトリのみにすることも、ルートディレクトリ以外のすべてのサービス提供者ディレクトリにすることも可能である。

【００９７】上記のように、スマートカードとの最も多数の交信はビジターユーザによるものである。これらの交信はフレキシブルにする必要があるが、用心深いものである必要もある。ＵＮＩＸオペレーティングシステムでは、ＰＡＴＨにないコマンドを実行しようとすることに対しては親切なメッセージが出るが、スマートカードは、許されないコマンドにアクセスしようとするこれらの試行を監視する必要がある。この場合も、カウンタを

使用して、事前に選択したカウントを超えた場合に、ビジターとの通信を終了し、メッセージをスマートカードに格納し、保有者以外の者に対してカードを無効にすることができる。保有者のディレクトリに格納されることになるそのメッセージは、中断した取引の詳細からなる。保有者が無許可コマンドを実行しようとした場合にも同様のアクションがあるが、その場合には診断メッセージがルート所有ファイルに書き込まれる。

【００９８】もう１つのセキュリティ手段は、ビジターによる正当な取引にも関係することがある。上記のように、ルートによって所有されるファイルのうちの１つにログファイルがあり、これはスマートカードによって実行されたすべての取引の記録を保持する。このファイルは、与えられた時間間隔に１つのビジターによってあまりに多くの取引があった場合、与えられた時間間隔にあまりに多くの取引があった場合などのような特定の状況が存在するようなときに、特定のビジターユーザまたはすべてのビジターユーザを許可しないようにチェックすることが可能である。

【００９９】スマートカードと交信する当事者はＯＫであるが、カードの所持者に問題がある場合には、わずかに異なるセキュリティ問題が生じる。この場合、スマートカードと対話している当事者は、その時点およびそれ以降では、スマートカードの使用を防止するのに協力したいと考えると容易に仮定される。これはいくつかの方法で実現される。例えば、ログインシーケンス中に所持者によって提示されたＩＤが（例えば、スマートカードが盗まれたものであるために）誤りである場合、商人はルートに属するファイルにメッセージを書き込むコマンドを実行しカードを無効にすることができる。この場合、カードを復元する唯一の方法はルートと交信することである。ルートがそのファイル内の診断メッセージを読んだ場合、所持者が実際は真の保有者であるか否かを判定し、適当なアクションをとることができる。

【０１００】スマートカードの上記の構造およびオペレーティングシステムが与えられると、スマートカード上のすべてのサービスをインストールする発行者／所有者がそれらのサービスの知識を有することは明らかである。すなわち、発行者／所有者は（スマートカードのルート所有者ではあるが）さまざまなサービス提供者によって所有されるファイル内を調べる能力を有しないが、それにもかかわらず、発行者／所有者は各スマートカード上にどのサービス提供者が存在するかについて知っている。この知識は、（各スマートカードが自分自身に関するそのような情報を保持することもできるが）発行者／所有者によって所有されるデータベースに保持することができる。

【０１０２】スマートカードを紛失しまたは破損した場合、すべてのサービス提供者を最初からインストールした新しいスマートカードを保有者に発行することができる。回復できない唯一の項目は、旧ファイル内にさまざまなユーザによって作成されたデータファイルと、サービス提供者のパスワードである。初期インストールについては、一時的なパスワードファイルのセットをインストールすることができる。その後、発行者／所有者はサービス提供者と交信して、一時パスワードについて通知し、保有者はサービス提供者と交信してそのパスワードを変更し、それぞれのディレクトリに必要なファイルを入れることができる。

【０１０３】［監査証跡］上記のように、ルートはログファイルを保持し、その中に各取引の記録を格納する。その後、このファイルは、保有者またはサービス提供者が課したいさまざまなしきい値を追跡するために使用することができる。

【０１０４】スマートカードの過度の使用は不正使用の表示の可能性がある。上記のように、このような使用は、ログファイルの注意深い監視によって検出することができ、それによって停止される。

【０１０５】しかし、ログファイルのもう１つの使用法として、完全に正当な使用に関するものも可能である。例えば、クレジット提供サービス提供者は、すべての小さい取引に対しては商人から「バッチ」送信（おそらくは就業日の終わりに）をさせながら、ある限界を超える負担を受ける場合には「リアルタイム」で通知してもらうことができる。スマートカードの電子財布に関して、保有者は、スマートカード内の金額値がある限界を下回った場合に保有者の銀行と自動的に交信し、さらに追加の資金をスマートカードに振り替えるように命令することができる。

【０１０６】監査証跡のさらにもう１つの使用法は、紛争解決に関するものである。商人が、スマートカードがある商品またはサービスを取得するために使用されたと主張し、保有者がその主張を争う場合、ログファイルは、その紛争を解決するために使用することができる。

【０１０７】［サービス提供者間の協力］サービス提供者が協力的提携をすることも全く可能である。このような提携は、スマートカードがアクセスされるときはいつでも、または、スマートカードが特定のユーザによってアクセスされるときに、スマートカードで実行されるさまざまな活動を指定することができる。このような可能性の数は無制限であり、以下の例は単なる例示のためのものである。

【０１０８】例えば、会社Ｚが、ガソリンをおそらくかなり定期的に購入する必要がある巡回販売員を雇用しているとする。Ｚは、Ｏと交信して、各販売員（保有者）にスマートカードを発行させ、Ｚをサービス提供者として、および、Ｇをガソリン提供者としてインストールするようにＯに要求する。しばらく後に、Ｚは、銀行Ｂと、販売員に対するクレジットの提供者として契約を結ぶ。このサービスは、例えばＧの協力を得ることによっ

23

て、販売員に属するすべてのスマートカードにリモートでインストールすることが可能である。

【０１０９】特に、Ｚは、スマートカードがＧと対話し、ＺがユーザであるがＢがユーザでないことを発見したときには、Ｏとの通信を要求するようインストールすることをＧに要求することができる。Ｇがする必要のあることは、Ｇで正しいスマートカードがログインしたときに適当なコマンドを送ることである。

【０１１０】上記の説明では「スマートカード」について述べたが、実際には、本発明は、人が行くところへはどこでも基本的にその人に伴って移動することを意図した任意の個人情報装置を考えている。すなわち、特許請求の範囲の意図としては、「スマートカード」という用語は、個人使用のために設計され、少なくともその機能のうちのいくつかは個人に関する情報を運搬することを意図したすべての装置を包含する。これは明らかに、例えば、セルラ電話機およびパーソナルコミュニケータを含む。これらは既に、本発明を実施することを可能にするのに必要な電子手段（例えば、プロセッサ）を有し、現在の期待は、人がこれらの電子装置を、通常クレジットカードを携帯するように、携帯するようになることである。

【０１１１】

【発明の効果】以上述べたごとく、本発明によれば、セ

24

キュリティの問題を克服し、リモート発給が可能であるような、複数のサービス提供者のサービスをのせたスマートカードが実現される。

【図面の簡単な説明】

【図１】ＵＮＩＸオペレーティングシステムの構造の図である。

【図２】スマートカードオペレーティングシステムのツリー構造の図である。

【図３】スマートカードとその発行者／所有者の間のログインプロトコルの図である。

【図４】スマートカード、その発行者／所有者およびサービス提供者に関わるプロトコルの図である。

【図５】スマートカードがサービス提供者からサービスを取得するプロトコルの図である。

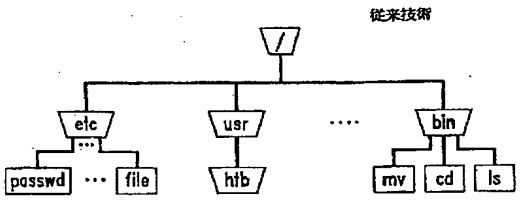
【図６】スマートカード、ビジターユーザおよびサービス提供者に関わるプロトコルの図である。

【図７】サービス提供者への接続のない、スマートカードとビジターユーザの間のプロトコルの図である。

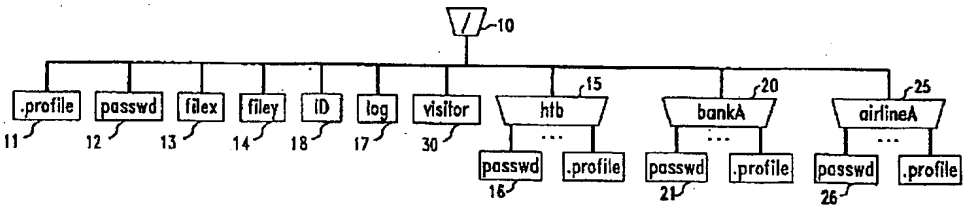
【図８】電気通信ネットワークを使用してスマートカードをリモート発給する配置の図である。

【図９】サービス提供者のファイルに記憶された値を引き出すオペレーティングシステムコマンドの流れ図である。

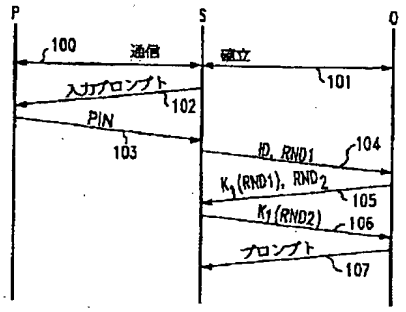
【図１】



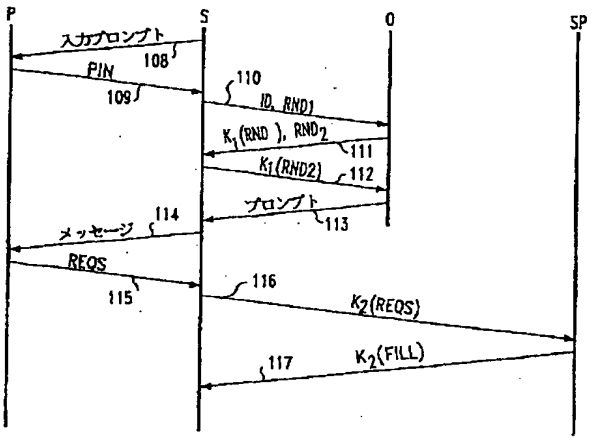
【図２】



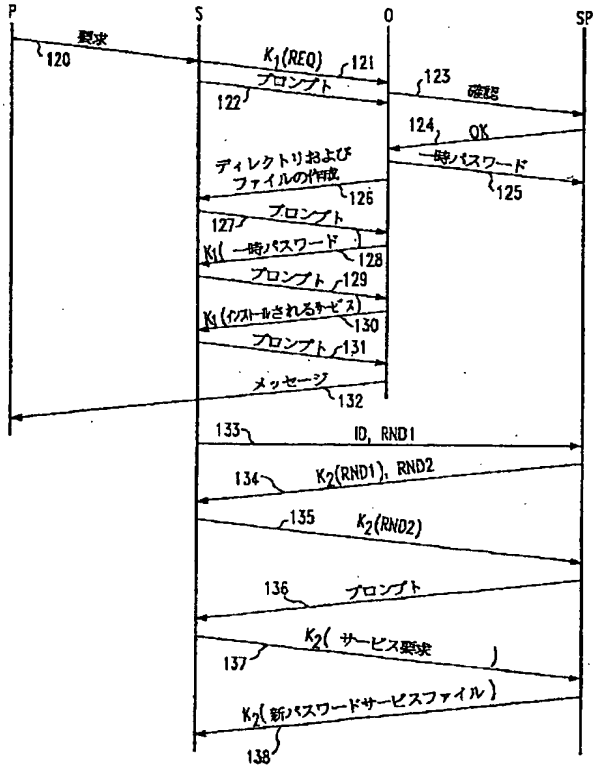
【図３】



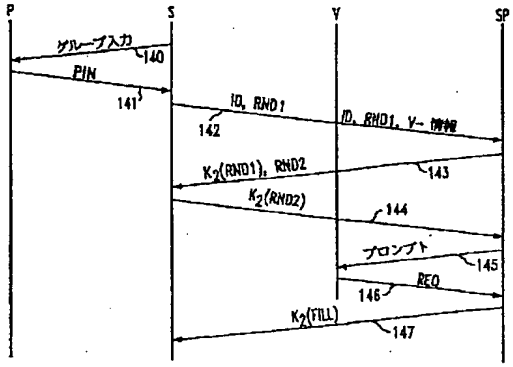
【図５】



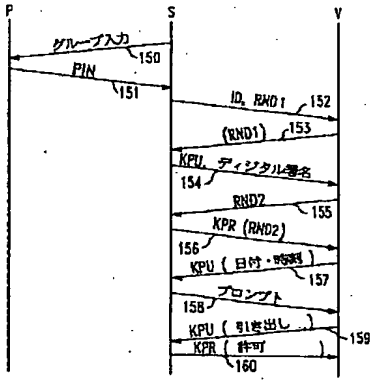
【図４】



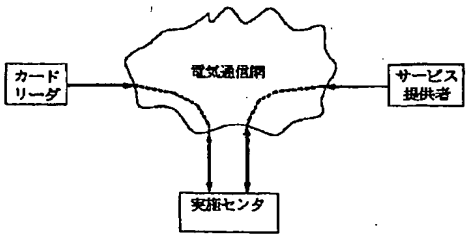
【図６】



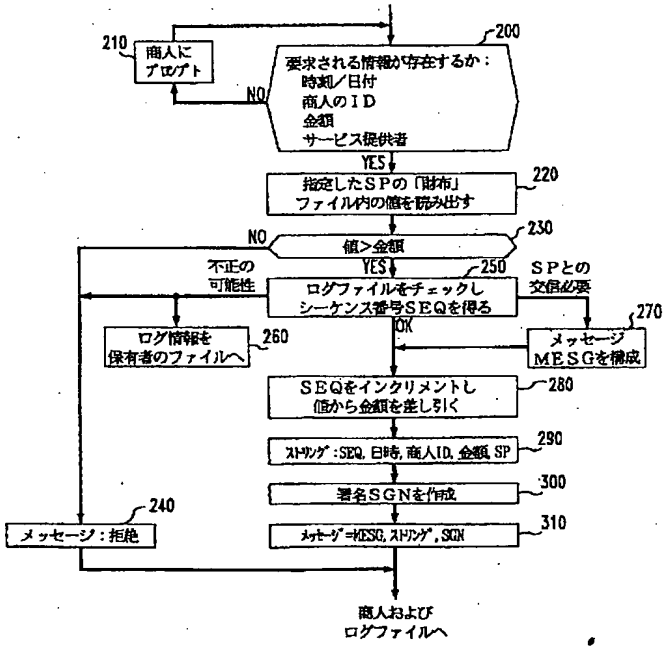
【図７】



【図８】



【図９】



フロントページの続き

(72)発明者　スティーヴン　アンドリュー　シャーマン
アメリカ合衆国、07840　ニュージャージー、ハケッツタウン、チャーチ　ストリート　206

(72)発明者　ダイアン　アール．ウェザリントン
アメリカ合衆国、07924　ニュージャージー、バーナーズヴィル、ウッドランド　ロード　28